System Security Group Project #2

(10% of class grade, due 2/9 at midnight)

Go through interactive broken web application tutorials. Explain what you learn! This project is worth 10% of your class grade.

What you will need:

You will need access to VirtualBox and the following virtual machine images:

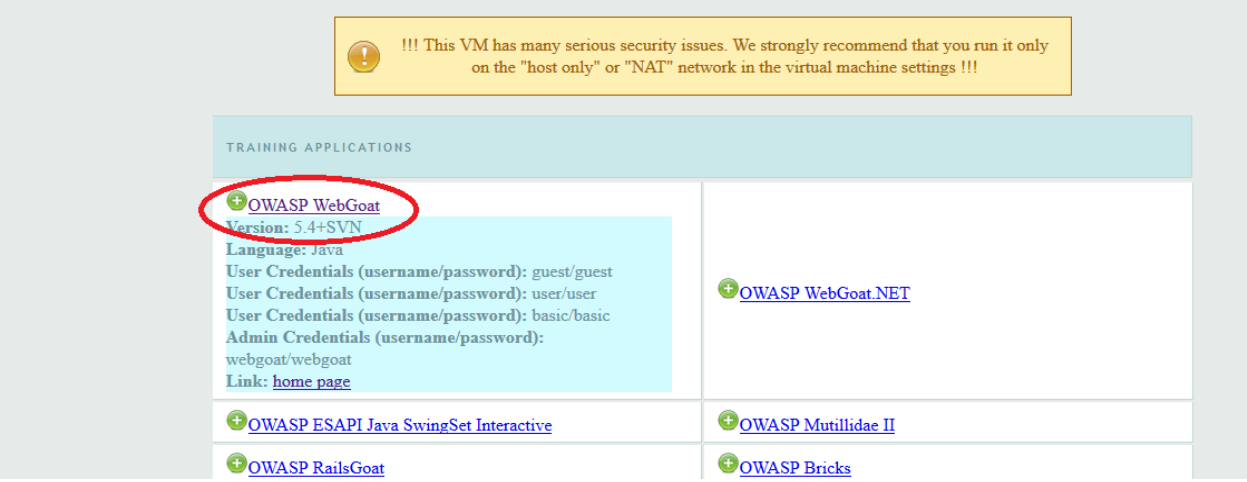
- OWASP-BWA
- Kali Linux (not mandatory if you are working on your own machine and can download/run the program webscarab and the preferred browser Firefox with Firebug or Dev Tools)

Directions:

Follow the in-class instructions for downloading and running the OWASP-BWA and the optional Kali Linux.

Start the OWASP-BWA image and log in with the given username/password combination. Open a browser either in your host computer or Kali Linux and navigate to the IP address given.

Select the OWASP WebGoat Link and log in with user/user to get going. (However, you should note the other user/pass combinations.)



"WebGoat is a deliberately insecure web application maintained by OWASP designed to teach web application security lessons. In each lesson, users must demonstrate their understanding of a security issue by exploiting a real vulnerability in the WebGoat applications. For example, in one of the lessons the user must use SQL injection to steal fake credit card numbers. The application aims to provide a realistic teaching environment, providing users with hints and code to further explain the lesson." – WebGoat wiki at https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project

On the left, click on the Introduction link. It will expand. Click on and read "How to work with WebGoat" and "Useful Tools". You can skip the part on Tomcat Configuration since it will already be set up for you.

Set up webscarab. Watch this video to set it up with Firefox on Kali Linux and to watch it in action. (Note the hacker-cool way the video has no sound…)

https://www.youtube.com/watch?v=C_3T_Y8QBFw

Lessons in WebGoat

Start with these first two lessons:

- General
- Insecure Storage

Then complete (as far as possible) at least 12 lessons out of the following:

- Access Control Flaws
- AJAX Security
- Authentication Flaws
- Buffer Overflows
- Code Quality
- Concurrency
- Cross-Site Scripting (XSS)
- Improper Error Handling
- Injection Flaws
- Denial of Service
- Insecure Communication
- Insecure Configuration
- Malicious Execution
- Parameter Tampering
- Session Management Flaws
- Web Services

The deliverable

I am expecting 2 parts to the deliverable.

1. **Paragraphs:** For each ***page of each module you complete***, type up at least one paragraph on what you learned. Don't just copy and paste text from the lesson plans (I will be checking). In your paragraph, let me know what was easy, what was hard, and what you couldn't get to work quite right. We will use class periods as work periods to ask questions about things you can't quite get and get advice from other teams. (All advice from other teams should get a citation/shout out in your paragraph.)
2. **Score cards:** In addition, go to Admin Functions -> Report Card and submit your score card(s) to me. Each group member should be participating. For example, if you split the project up into three equal pieces, each member should submit a score card. If you all worked together on all the activities, just submit one score card. If you worked together on some things *and*

individually other things, you will need to make clear who did what and submit all the score cards.

Your deliverable should be on your team wiki. Create a new page called "WebGoat" directly under your main team wiki page and place your paragraphs and score cards in there.

In addition, you will be required to fill out a blackboard survey on the distribution of work before you get a grade. (You cannot skip this part.)

Other Things

- I do not have all the answers. (I know, I look like I do…)
- I'm expecting things to sometimes be difficult, even with the hints and solution videos available. Sometimes the difficulty will be in getting things set up. Other times it might be in figuring out what you should be watching or modifying.
- If you don't know what something is, Google it to find out!
- I expect you to have to use Google to figure out features of webscarab or firebug.
- I know other walkthroughs exist on the Internet. If you use another source, cite it!
- Make sure you are taking the time to learn. If your paragraphs don't convince me you really understand what's going on, I will award less points.